ALASKA'S EXPLICIT RIGHT TO PRIVACY WARRANTS GREATER PROTECTION OF ALASKANS' PERSONAL DATA

*Eric Buchanan**

ABSTRACT

Alaska's legislature should pass a comprehensive data privacy law to prevent companies' exploitation of citizens' personal data. The Alaska Constitution explicitly provides Alaskans with the right to privacy and calls upon the legislature to protect that right. Despite this explicit right, Alaskans' privacy rights are vulnerable to exploitation by private companies. Proposed legislation to address this vulnerability should ensure data privacy protection, but the legislature should remain cognizant of concerns regarding innovation and business. To best achieve this balance, the legislation should be founded in generally accepted data privacy principles and should establish strong financial penalties for companies that violate the law. The legislation should also be flexible enough to avoid stifling innovation and unreasonably increasing compliance costs. More specifically, the law should allow companies to provide financial incentives to consumers in exchange for permission to collect, use, and share their data. Privacy legislation that meets these goals will effectively protect data privacy, while simultaneously enabling companies to innovate and turn a profit.

* J.D., Duke University School of Law, 2020; B.A., Political Science and Spanish, State University of New York (SUNY) at Geneseo, 2016. The author would like to thank Professor Rebecca Rich and the *Alaska Law Review* Staff for their guidance and comments throughout the drafting of this Note. The views expressed, along with any omissions or errors, remain the author's own.

> *"[S]ome of the most prominent and successful companies have built their businesses by lulling their customers into complacency about their personal information. They're gobbling up everything they can learn about you and trying to monetize it. We think that's wrong."*
>
> – Tim Cook, Apple CEO[1]

I. INTRODUCTION

Personal data has become a lucrative commodity, generating billions of dollars for the private companies that collect it.[2] Data's value is derived from its versatility—it can be used to improve the customer experience, refine marketing strategy, generate cash flow, drive business decisions, promote product development, and even secure additional data.[3] Data-driven innovation has revolutionized the way individuals interact with the world, offering services that make everyday life more convenient. However, "with prodigious potential, comes prodigious risk."[4]

Today, private companies collect information regarding shopping habits, religious affiliations, sexual preferences, and personal relationships, as well as locational and sensitive health data.[5] All this data, with few sector-specific exceptions,[6] can be used however the company wishes.[7] The lack of regulation is concerning: the sensitive nature of this

1. LEANDER KAHNEY, TIM COOK: THE GENIUS WHO TOOK APPLE TO THE NEXT LEVEL 167 (2019).

2. MICHAEL CHERTOFF, EXPLODING DATA: RECLAIMING OUR CYBER SECURITY IN THE DIGITAL AGE 77 (2018). To further understand the value of data, consider another quote by Apple CEO Tim Cook: "Every day, billions of dollars change hands and countless decisions are made on the basis of our likes and dislikes, our friends and families, our relationships and conversations, our wishes and fears, our hopes and dreams. These scraps of data, each one harmless enough on its own, are carefully assembled, synthesized, traded and sold." *Tim Cook: Personal Data Collection is Being 'Weaponized Against Us with Military Efficiency,'* CNBC (Oct. 24, 2018), https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html.

3. *See generally* Adam C. Uzialko, *How Businesses are Collecting Data (And What They're Doing With It)*, BUS. NEWS DAILY (Aug. 3, 2018), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

4. Zynep Tufekci, *We're Building a Dystopia Just to Make People Click on Ads*, TEDTALK (1:51) (Oct. 27, 2017), https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads.

5. CHERTOFF, *supra* note 2, at 73.

6. Entities that must comply with at least some privacy-specific regulations are healthcare, banking, and credit reporting companies, and companies that knowingly collect children's data. *See infra* Section III.C.

7. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 3 TEX. L. REV. 85, 146 (2014) (explaining how the FTC can pursue privacy violations when the company has

data can result in the denial of medical insurance, unfavorable employment decisions, discriminatory ad targeting, and other forms of discrimination.[8] Furthermore, a company that collects data during its regular course of business can sell it to whichever commercial, ideological, or political actor is willing to pay.[9] Malicious actors can also gather detailed intelligence on specific individuals and use that data to undermine the integrity of elections, radicalize and recruit vulnerable populations, and disseminate false information.[10]

A comprehensive privacy regime could safeguard citizens against malicious uses of data by providing people with greater control over their personal information and by encouraging companies to implement internal consumer data protections. However, the United States' current federal privacy regime fails to adequately protect consumer data,[11] and it seems unlikely that Congress will pass comprehensive federal privacy legislation any time in the near future.[12] Therefore, legislation protecting Alaska citizens from potential exploitation should come from Alaska's government.

The potential exploitation of Alaska resources is not a novel problem. The trend of data exploitation, although not unique to Alaska, is strikingly similar to the exploitation of natural resources that Alaska has previously confronted. Alaska's abundance of natural resources has resulted in both economic booms and busts throughout its history.[13] Outsiders have flocked to Alaska, seeking to profit from these valuable resources only to leave once they have made their fortunes.[14] These economic booms contributed to Alaska's growth. However, the economic

deceptive or misleading privacy policies).

8. *See infra* Section III.A.

9. *See* CHERTOFF, *supra* note 2, at 42 (describing the utility of data).

10. DONALD J. TRUMP, NATIONAL SECURITY STRATEGY OF THE UNITED STATES 31–35 (2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

11. *See infra* Section III.C.

12. This is largely because of the presidential impeachment hearing, the looming 2020 elections, and Congress's general inability to pass legislation. *See Trump Impeachment: A Very Simple Guide*, BBC (Dec. 19, 2019), https://www.bbc.com/news/world-us-canada-39945744 (summarizing the Trump impeachment proceedings); *see also* Drew Desilver, *A Productivity Scorecard for the 115th Congress: More Laws Than Before, But Not More Substance*, PEW RESEARCH CTR. (Jan. 25, 2019), https://www.pewresearch.org/fact-tank/2019/01/25/a-productivity-scorecard-for-115th-congress/ (noting that the current Congress is one of the least productive in history).

13. *See* ERIC SANDBERG, ALASKA DEPT. LABOR & WORKFORCE DEV., A HISTORY OF ALASKA POPULATION SETTLEMENT 9–12, 15–16 (Sara Whitney ed., 2013) (discussing the economic booms and busts resulting from gold and oil discoveries).

14. *Id.*

busts forced Alaskans to consider how to utilize resources to drive economic growth while simultaneously preventing exploitation.[15]

In their effort to address this issue, Alaskans have made a conscious effort to mitigate those risks. Alaska's statehood movement was spurred largely by concerns over control of Alaska's natural resources.[16] Many pre-statehood residents traced the exploitation of Alaska's resources "to [the] sins of omission and commission by the federal government."[17] They believed the only way that residents could regain control of fish and wildlife, minerals, forests, and other resources was through statehood.[18] Accordingly, the framers incorporated these basic objectives into the Alaska Constitution by adding a section dedicated to the protection of natural resources.[19] And in the following decades, Alaska learned from the experiences during pre-statehood and used its constitution as inspiration to find solutions addressing new threats to the state's natural resources.[20]

Once again outsiders are exploiting Alaska's resources and taking the profits for themselves. Much like the exploitation in the past, this recurrence can be attributed to "sins of omission and commission by the federal government."[21] The lack of federal legislation protecting data privacy on a national scale enables this exploitation. However, Alaska's government has the explicit authority to mitigate these risks and protect

15. GORDON HARRISON, ALASKA LEGISLATIVE AFFAIRS AGENCY, ALASKA'S CONSTITUTION: A CITIZEN'S GUIDE 129–30 (5th ed. 2012), http://w3.legis.state.ak.us/docs/pdf/citizens_guide.pdf (discussing the legislative history surrounding the inclusion of natural resource rights under the Alaska Constitution).

16. GERALD A. MCBEATH & THOMAS A. MOREHOUSE, ALASKA POLITICS & GOVERNMENT 126 (1994).

17. *Id.*

18. *See* HARRISON, *supra* note 15, at 129–30 (explaining the legislative history surrounding the passage of article VIII of the Alaska Constitution).

19. *Id.*; *see also* ALASKA CONST., art. VIII, § 3 ("Wherever occurring in their natural state, fish, wildlife, and waters are reserved to the people for common use."); ALASKA CONST., art. VIII, § 15 ("No exclusive right or special privilege of fishery shall be created or authorized in the natural waters of the State. This section does not restrict the power of the State to limit entry into any fishery for purposes of resource conservation, to prevent economic distress among fishermen and those dependent upon them for a livelihood and to promote the efficient development of aquaculture in the State."). The second part of section 15 was added through a 1972 amendment to authorize an exception to the first sentence's prohibition, allowing the state to institute a limited entry program for distressed fisheries. HARRISON, *supra* note 15, at 38.

20. *See, e.g.*, ALASKA STAT. §§ 46.03.010–46.03.045 (2018) (implementing policies regarding environmental conservation); *id.* §§ 46.11.020–46.11.070 (implementing policies regarding conservation of energy and materials); *id.* § 46.35.300 (discussing the extension of resource extraction or removal related permits).

21. *See* MCBEATH & MOREHOUSE, *supra* note 16.

Alaskans. Unlike the United States Constitution, the Alaska Constitution expressly provides its citizens with the right to privacy.[22] Despite this explicit right, Alaska does not currently afford data privacy protection above the minimum federal protection.[23]

The Alaska Supreme Court has relied on Alaska's constitutional right to privacy to protect Alaska citizens from privacy intrusions by the government; however, it has refused to extend these protections to violations perpetrated by private companies.[24] Thus, in order to protect its citizens from such violations, the Alaska legislature should pass comprehensive privacy legislation. This law should borrow key aspects from California's and the European Union's comprehensive privacy regulations.

This Note proceeds in four parts. Part II will describe Alaska's explicit right to privacy and explain how Alaska's interest in privacy has hindered greater data protection. Part III will justify why the legislature should pass comprehensive privacy legislation. It will specifically focus on the harms associated with unregulated data usage, tort law's inability to adequately protect data privacy, the lack of federal comprehensive privacy legislation, and the benefits that would be provided through comprehensive data privacy legislation. Part IV will discuss how American values generally and Alaskan values specifically change the calculus of what should be included within the act. Finally, Part V will explain key elements that the legislature should include within the bill, borrowing various ideas from the European Union's General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA).

II. ALASKA'S EXPLICIT RIGHT TO PRIVACY AND THE COURT'S INABILITY TO SUFFICIENTLY PROTECT IT

This Section will proceed by first briefly explaining Alaska's longstanding tradition of protecting individuality and privacy. Specifically, it will discuss Alaska's explicit right to privacy and how the court has interpreted the constitutional privacy protection with regard to data privacy. It will also describe the limitations on the court's powers and explain why the legislature must be the branch to protect Alaska citizens from data exploitation by private companies.

22. *See* ALASKA CONST., art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.").
23. *See infra* Part II.
24. *See infra* Section II.B.

A. Alaska's Tradition of Respecting Privacy and Individuality

Alaska has a longstanding tradition of respecting privacy and individuality.[25] Many of Alaska's early settlers were escaping various forms of misfortune, trouble, and misconduct.[26] Others simply found life too constricting within developed cities and communities of the lower forty-eight and sought refuge at the edge of the frontier.[27] The Alaska Supreme Court has recognized this uniqueness, stating that:

> [O]ur territory and now state has traditionally been the home of people who prize their individuality and who have chosen to settle or to continue living here in order to achieve a measure of control over their own lifestyles which is now virtually unattainable in many of our sister states.[28]

These characteristics have evolved into Alaska's general policy of tolerance towards personal idiosyncrasy, unconventional lifestyle and thought, and personal privacy.[29]

Demonstrating the importance of individuality and privacy to Alaskans, Alaska is only one of eleven states[30] with an explicit right to privacy in its constitution.[31] Article I, section 22 of the Alaska Constitution declares that "[t]he right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section."[32] Section 22 was added to the constitution by an amendment in 1972 in response to the development of a computerized database of information on the criminal history of individuals.[33] The legislature feared that such a system would result in privacy intrusions reminiscent of a "Big Brother" government surveillance regime leading to the constitutional

25. Susan Orlansky & Jeffrey M. Feldman, *Justice Rabinowitz and Personal Freedom: Evolving a Constitutional Framework*, 15 ALASKA L. REV. 1, 1 (1998).

26. *Id.*

27. *Id.*

28. Ravin v. State, 537 P.2d 494, 504 (Alaska 1975).

29. Orlansky & Feldman, *supra* note 25, at 1.

30. The other ten states that have explicit rights to privacy in their constitutions are Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, New Hampshire, South Carolina, and Washington. *Privacy Protections in State Constitutions*, NAT'L CONFERENCE OF STATE LEGISLATURES (Nov. 7, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

31. *Id.*

32. ALASKA CONST., art. I, § 22.

33. HARRISON, *supra* note 15, at 38. In 1971, the FBI implemented a computerized system called the Computerized Criminal History ("CCH") Program. U.S. DEP'T OF JUSTICE, USE AND MANAGEMENT OF CRIMINAL HISTORY RECORD INFORMATION: A COMPREHENSIVE REPORT 49 (1992), https://www.bjs.gov/content/pub/pdf/CCHUSE.PDF. The CCH held the full criminal history records for both federal offenders and state offenders from participating states. *Id.*

amendment's proposal and ratification.[34]

Although the legislative history specifically reflects concerns about the government controlling vast amounts of data on individuals, it also suggests a broader concern about large amounts of data in the hands of powerful entities. It is unlikely that the legislators at the time of the 1972 amendment could have imagined the situation of today—private companies collecting, controlling, using, and selling data as personal as geolocational or medical information. However, the language of the amendment itself depicts a remarkable level of foresight, explicitly directing the Alaska legislature—the most flexible and representative branch of government—to pass legislation to protect Alaska citizens' privacy.[35]

Despite the Alaska Constitution's explicit call for the legislature to implement the right to privacy, the legislature has been reluctant to act within the data privacy sphere.[36] Only one law exists that even tangentially addresses data privacy: the Personal Information Protection Act,[37] which specifically pertains to data breaches.[38] However, the law provides no guidance on how private companies should collect, store, use, or protect consumer data; it simply requires companies to notify consumers of a breach.[39] Due to the legislature's inaction, the Alaska Supreme Court has largely carried out the implementation, development, and protection of this right.

B. Limitations on the Court's Powers to Regulate Privacy Violations

State courts may interpret state constitutional provisions independent of federal law when those provisions lack a federal constitutional equivalent, such as Alaska's explicit right to privacy.[40] The

34. HARRISON, *supra* note 15, at 38. The delegates to the constitutional convention sixteen years earlier were also concerned about technological intrusion into the lines of ordinary citizens' lives; however, that fear was limited to wiretapping and electronic surveillance. *Id.* The delegates considered, but ultimately rejected, including the following language in the constitution's unreasonable searches and seizures section: "The right of privacy of the individual shall not be invaded by use of any electronic or other scientific transmitting, listening or sound recording device for the purpose of gathering incriminating evidence. Evidence so obtained shall not be admissible in judicial or legislative hearings." *Id.*

35. *See* ALASKA CONST., art. I, § 22 ("The legislature shall implement this section.").

36. *See infra* Section III.A.

37. Personal Information Protection Act, ALASKA STAT. §§ 45.48.010–995 (2018).

38. *See generally id.*

39. *See generally id.*

40. Jeffrey M. Shaman, *Eighteenth Annual Issue on State Constitutional Law:*

Alaska Supreme Court has done precisely that, and has as a consequence expanded Alaska citizens' privacy rights beyond those of citizens elsewhere in the United States. The court has stated:

> Since the citizens of Alaska, with their strong emphasis on individual liberty, enacted an amendment to the Alaska Constitution expressly providing for a right to privacy not found in the United States Constitution, it can only be concluded that the right is broader in scope than that of the Federal Constitution.[41]

Reflecting this willingness to expand Alaskans' right to privacy beyond the federally recognized right to privacy, the court has recognized that medical marijuana users have an interest in keeping their usage and medical condition private;[42] that police officers have legitimate expectations of privacy regarding their personnel files;[43] that a statute requiring a person who places a political advertisement in a newspaper "reveal his name, address, occupation, employer, and the amount of his expenditure" burdens his right to privacy;[44] and most recently, that sex offenders have a legitimate expectation of privacy in preventing the widespread publication of their conviction and personal information.[45]

Despite touting privacy rights in the aforementioned situations, the Alaska Supreme Court has been reluctant to expand data privacy rights to actions perpetrated by private actors. In *Luedtke v. Nabors Alaska Drilling*,[46] the supreme court addressed whether Alaska's constitutional right to privacy could be applied to private actors.[47] The court explicitly refused to extend constitutional protections to private actors' privacy violations.[48] The court noted that article I, section 22 failed to provide guidance on how the right should be applied, and that the legislature had not exercised its power pursuant to article I, section 22.[49] The court explained that the primary purpose of the constitutional right to privacy is to protect "personal privacy and dignity against unwarranted

Article: The Right of Privacy in State Constitutional Law, 37 RUTGERS L.J. 971, 988 (2006).

41. Ravin v. State, 537 P.2d 494514–15 (Alaska 1975) (Boochever, J., concurring).

42. Rollins v. Ulmer, 15 P.3d 749, 752–53 (Alaska 2001).

43. Jones v. Jennings, 788 P.2d 732, 738 (Alaska 1990).

44. Messerli v. State, 626 P.2d 81, 86 (Alaska 1980).

45. Doe v. Dep't of Pub. Safety, 444 P.3d 116, 128 (Alaska 2019).

46. 768 P.2d 1123 (Alaska 1989).

47. *Id.* The precedent set in *Luedtke* remains controlling. *See* Miller v. Safeway, 102 P.3d 282, 287–88 (Alaska 2004) (utilizing *Luedtke* to support the assertion that an Alaskan's right to privacy cannot be violated without state action).

48. *Luedtke*, 768 P.2d at 1129.

49. *Id.*

intrusions by the State."[50] However, within the same analysis, the court recognized constitutional clauses in other jurisdictions that prohibit private action, leaving open the possibility that Alaska's constitutional right to privacy could be applied to private action.[51] Despite acknowledging this possibility, the court refused to extend the right to privacy to the private actions involved in the case.[52] The court explained that the plaintiff had failed to provide evidence that Alaska's constitutional right to privacy was intended to apply to private actors.[53]

Thus, the precedent set in *Luedtke* and the general lack of evidence regarding the constitutional amendment's drafters' intent make it unlikely that the court will protect citizens from privacy violations perpetrated by private actors. If Alaska wants to protect its citizens from privacy violations by private companies, then the legislature must be the branch to act. Importantly, article I, section 22 of the Alaska Constitution explicitly calls on the legislature to act. Therefore, the Alaska legislature should draft a comprehensive privacy bill to carry out its responsibilities by protecting its citizens' privacy.

III. WHY THE ALASKA LEGISLATURE SHOULD PASS COMPREHENSIVE PRIVACY LEGISLATION

This Section will explain why the Alaska legislature should pass comprehensive privacy legislation. It will first discuss how data can be used to harm Alaska citizens. It will then describe how tort law insufficiently protects data privacy. Next, it will describe the current federal data privacy regime and its deficiencies. Then, it will explain the potential benefits to companies that could result from comprehensive federal privacy legislation.

A. The Misuse of Data Can Harm Citizens

Data is valuable because it can be used to predict and assess behavior, to facilitate better-informed business decisions, and to increase revenue.[54] The more data a company has, the more accurate its

50. *Id.*
51. *Id.* at 1129–30.
52. *Id.* at 1130.
53. *Id.* The court further explained that "absent a history demonstrating that the amendment was intended to proscribe private action, or a proscription of private action in the language of the amendment itself, we decline to extend the constitutional right to privacy to the actions of private parties." *Id.*
54. *See* John Akred & Anjali Samani, *Your Data is Worth More Than You Think*, MIT SLOAN (Jan. 18, 2018), https://sloanreview.mit.edu/article/your-data-is-worth-more-than-you-think/.

predictions will be.[55] Thus, companies are incentivized to collect as much data as possible on consumers.[56]

Consumer data can be used for benign purposes such as marketing or improving products.[57] However, the data can also be used for discriminatory purposes, whether it be intentional or unintentional. For example, health insurance companies can collect and use unprotected sensitive health information to make coverage decisions by incentivizing voluntary disclosure through reduced rates and rewards, or by purchasing it from fitness tracking companies.[58] The data collected through these mechanisms are not protected by federal privacy laws and can be used to predict an individual's risk of a significant medical event.[59] The results of the risk assessment will inform a company's decision on whether to cover that individual—unhealthy or high-risk individuals could be denied coverage. The health insurance company that denies coverage could then sell the individual's data to other health insurance companies, ensuring that the individual cannot obtain health insurance, all because of potentially flawed predictions of medical risk unconfirmed by a medical professional.

Another possible discriminatory use includes employers who build algorithms to uncover statistical relationships in data sets of potential employees.[60] The use of such algorithms, though efficient, can cause classification bias—employer reliance "on classification schemes, such as data algorithms, to sort or score workers in ways that worsen inequality or disadvantage along the lines of race, sex, or other protected characteristics."[61] Additionally, targeted ads can be discriminatory. For

55. Sarah Littler, *The Importance and Effect of Sample Size*, SELECT STATISTICAL SERVS., https://select-statistics.co.uk/blog/importance-effect-sample-size/ (last visited Nov. 19, 2019).

56. *Id.*

57. Louis Columbus, *Ten Ways Big Data Is Revolutionizing Marketing And Sales*, FORBES (May 9, 2016), https://www.forbes.com/sites/louiscolumbus/2016/05/09/ten-ways-big-data-is-revolutionizing-marketing-and-sales/#2f9cc0721cff.

58. In 2018, an insurance company, John Hancock, announced that all of its policies would come with the option to let the company track your fitness through its website or a fitness tracker like Fitbit. Christopher Ingraham, *An Insurance Company Wants You to Hand Over Your Fitbit Data so it Can Make More Money. Should You?*, WASH. POST (Sept. 25, 2018), https://www.washingtonpost.com/business/2018/09/25/an-insurance-company-wants-you-hand-over-your-fitbit-data-so-they-can-make-more-money-should-you/. This program would come with lower rates and rewards for meeting fitness goals, which seems great for healthy customers. *Id.*

59. *See infra* Section III.C.

60. Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 865 (2017).

61. *Id.* at 866. Consider a company called Gild, which offers a "smart hiring platform" to assist companies in finding "the right talent quicker." *Id.* at 862.

example, a bank could target individuals who post information online about recently losing their job because they are considered a likely candidate for a high-interest loan.[62] These individuals are targeted because they fall within the category of people the bank is attempting to reach, despite the fact that the person might qualify for a much lower rate.[63]

Furthermore, a company's client list is largely protected from public disclosure, making it difficult to hold companies accountable for the entities to which they sell information.[64] Thus, malicious actors can obtain consumer data from legitimate businesses and use it to radicalize and recruit individuals and to disseminate false information.[65] This nefarious use of data was exemplified through the Russian interference in the 2016 presidential election. The Internet Research Agency (IRA)—a private organization, with ties to the Russian government—successfully engaged in a misinformation campaign designed to cause instability and to influence the 2016 election.[66] The IRA directly engaged with tens of millions of Americans, targeting particularly vulnerable subsections of the population, to spark controversy and sow discord among Americans.[67]

Guild's algorithm analyzes thousands of pieces of information to calculate "around 300 larger variables about an individual: the sites where a person hangs out; the types of language, positive or negative, that he or she uses to describe technology of various kinds; self-reported skills on LinkedIn; [and] the projects a person has worked on, and for how long," as well as traditional criteria such as college major and education. *Id.*

62. *White House Says Big Data Can be Used to Discriminate Against Americans*, NPR (Apr. 26, 2014), https://www.pbs.org/newshour/nation/white-house-says-big-data-used-discriminate-americans. A person who lost his job is more likely to fall behind on his mortgage and thus might be more willing to accept a high-interest loan to catch up. *Id.*

63. *Id.*

64. Matthew Crane, *The Limits of Transparency: Data Brokers and Commodification*, 20 NEWS MEDIA & SOC'Y 88, 94 (2018), https://journals.sagepub.com/doi/pdf/10.1177/1461444816657096 ("Congress has largely failed to compel data brokers to identify information sources and clients.").

65. TRUMP, *supra* note 10, at 12–13, 31–35 (describing how information can be used to harm the United States and its citizens).

66. ROBERT S. MUELLER, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 4 (2019), https://www.justice.gov/storage/report.pdf.

67. *Id.* Facebook's General Counsel estimated that "roughly 29 million people were served content in their News Feeds directly from the IRA's 80,000 posts over the two years." *Social Media Influence in the 2016 U.S. Election, Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 5 (2017) (testimony of Colin Stretch, General Counsel, Facebook). However, because these posts were also shared, liked, and followed by people on Facebook, he believed that three times more people might have been indirectly exposed to a story posted by the IRA. *Id.* Stretch

Additionally, technology has also granted non-state actors military and political capabilities that were previously inconceivable. Specifically, the Internet and data aggregation has greatly expanded terrorist and radical groups' ability to recruit.[68] Today, terrorist and radical organizations no longer aimlessly recruit on a quantitative basis.[69] Instead, these groups engage in misinformation and propaganda campaigns similar to those carried out by the Russians during the 2016 election.[70] Data allows these groups to send specific messages to a target population based on a certain set of values, preferences, and demographic attributes.[71] The Internet generally and social media specifically provides the perfect medium to radicalize and recruit individuals.[72] The Internet provides anonymity and a degree of protection from detection that allows individuals to exhibit behaviors and attitudes that would be unacceptable in the physical world.[73] Additionally, the Internet can act as an echo chamber, where potential recruits are flooded with material focused on their preferences.[74] Exposure to differing viewpoints and opinions is more difficult to encounter.[75] Thus, terrorist and radical organizations can effectively normalize radical beliefs in potential recruits by using the Internet and data obtained from private companies.[76]

Due to data's potential to facilitate discrimination and to be weaponized against the citizenry, the Alaska legislature should pass a law requiring private companies to reasonably protect consumer data. Comprehensive data privacy legislation will promote better data practices that reduce the possibility that data will be used for

estimated that approximately 126 million people might have received content from an IRA-associated page at some point during the two-year period. *Id.*

68. GABRIEL WEIMANN, U.S. INST. OF PEACE, WWW.TERROR.NET: HOW MODERN TERRORISM USES THE INTERNET 6–7 (2004); *see also* Martin Rudner, *"Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror*, 40 STUDIES IN CONFLICT & TERRORISM 10, 10 (2017); *see also* INES VON BEHR *ET AL.*, RADICALISATION IN THE DIGITAL ERA: THE USE OF THE INTERNET IN 15 CASES OF TERRORISM AND EXTREMISM xii (2013), https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf.

69. WEIMANN, *supra* note 68.

70. UNITED NATIONS OFFICE ON DRUGS AND CRIME, THE USE OF THE INERNET FOR TERRORIST PURPOSES 3–5 (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

71. *Id.*; WEIMANN, *supra* note 68; *see e.g.,* Rudner, *supra* note 68, at 12.

72. *See* WEIMANN, *supra* note 68. The process entails direct contact with the individual, but also indirect contact such as promulgating false stories that provide a false sense of validation in the vulnerable individual. *See id.* at 144 (explaining how hackers can shape an individual's viewpoint).

73. INES VON BEHR, *supra* note 68, at 18.

74. *Id.*

75. *Id.*

76. *Id.*

discriminatory purposes or accessed by malicious actors.

B. Current State Tort Law Provides Insufficient Protection Against Privacy Violations

Currently, tort law is the only remedy that Alaskans have against private actors that violate their privacy rights. There are four privacy torts that states generally recognize:[77] (1) intrusion upon seclusion;[78] (2) public disclosure of private fact;[79] (3) false light;[80] and (4) misappropriation.[81] Alaska, however, only recognizes two of these four torts: false light[82] and intrusion upon seclusion.[83] Neither of these torts sufficiently protects individual privacy against private companies' misuses.[84] Specifically, false light requires that the false depiction of the plaintiff would be "highly offensive to a reasonable person" and that the plaintiff "had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."[85] The highly offensive requirement is difficult to establish in the context of corporate use of personal data. Companies often collect, use, and disseminate information in bits and pieces, frequently involving relatively innocuous information that fails to be highly offensive when each act is taken separately.[86] Thus, few plaintiffs will be able to succeed on a false light cause of action against a company's use of their personal data.

The tort of intrusion upon seclusion is also insufficient to protect an

77. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (dividing privacy torts into four distinct torts).

78. Intrusion upon seclusion is the "[i]ntrusion upon the plaintiff's seclusion or solitude, or into his private affairs." Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1889–90 (2010).

79. Public disclosure of private fact is the "[p]ublic disclosure of embarrassing private facts about the plaintiff." *Id.*

80. False light is "[p]ublicity which places the plaintiff in a false light in the public eye." *Id.*

81. Misappropriation is the "[a]ppropriation, for the defendant's advantage, of the plaintiff's name or likeness." *Id.*

82. *See* State v. Carpenter, 171 P.3d 41, 53, n.21 (Alaska 2007) (adopting the RESTATEMENT (SECOND) OF TORTS' description of a false light claim).

83. *See* Greywolf v. Carroll, 151 P.3d 1234, 1244–45 (Alaska 2007); Eli A. Meltz, *No Harm, No Foul? "Attempted" Invasion of Privacy and the Tort of Intrusion Upon Seclusion*, 83 FORDHAM L. REV. 3431, 3440 (2015).

84. In fact, "it is becoming increasingly clear that the common law invasion of privacy torts [in general] will not help to contain the destruction of [data] privacy."84. Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, 89 GEO. L. J. 2029, 2043 (2001).

85. *Carpenter*, 171 P.3d at 53, n.21.

86. Richards & Solove, *supra* note 78, at 1919.

individual's data privacy.[87] Intrusion upon seclusion requires an entity to "*intentionally* intrude[], physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns."[88] Two elements must be met for the plaintiff to succeed: (1) the plaintiff has a reasonable expectation of privacy, and (2) the defendant's manner of intrusion was highly offensive to a reasonable person.[89] The plaintiff is unlikely to establish a reasonable expectation of privacy in the context of corporate collection of personal data. Much of the data collected and used by private companies originates from the public domain or is voluntarily provided to the company in exchange for services, and courts have concluded that the collection and use of such data does not invade a person's privacy.[90]

Even if a consumer succeeds in overcoming these procedural hurdles, the tort system in general is still flawed. First, it is difficult to establish standing in a case alleging a privacy tort. To establish standing, a plaintiff must prove three elements: "(1) an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision."[91] To establish injury in fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[92] Mere procedural violations are insufficient to constitute an injury in fact.[93] Normally, a company's sale or use of an individual's personal data does not result in a provable particularized injury.[94] Thus, plaintiffs alleging a privacy violation face an uphill battle establishing standing.

87. *Id.*
88. *Greywolf*, 151 P.3d at 1244–45.
89. *Id.* at 1245.
90. Richards & Solove, *supra* note 78, at 1919. Individuals generally do not have a reasonable expectation of privacy in documents or information that is voluntarily provided to and maintained by a third party because those individuals have neither ownership nor possession of that information—commonly known as the third-party doctrine. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (finding no legitimate expectation of privacy in information voluntarily turned over to third parties); United States v. Miller, 425 U.S. 435, 440–41 (1976) (holding that the plaintiffs had no reasonable expectation of privacy in bank records because they had neither ownership nor possession of the documents).
91. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
92. *Id.* at 1548 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).
93. *Id.* at 1550.
94. *See* Lee J. Plave & John W. Edson, *First Steps in Data Privacy Cases: Article III Standing*, 37 FRANCHISE L.J. 485, 489 (2018) ("In many data breach lawsuits, plaintiffs who have had their personal data compromised are unable to prove that they are actually the victim of fraud or have suffered any tangible economic loss. Instead, these plaintiffs generally argue that, because of the data beach, they are at a greater risk of future identity theft or other harm.").

Additionally, the action of filing suit will likely bring more attention to an already sensitive issue. An individual will have to relive the embarrassment of the initial privacy invasion by discussing it in a public hearing and having the information entered into public record.[95] Finally, it is extremely difficult to recover substantial monetary damages from privacy tort lawsuits, shifting a plaintiff's cost-benefit analysis further away from filing suit in the first place.[96] Thus, the privacy tort system inadequately addresses the modern privacy problems associated with the collection, use, and dissemination of consumer data.

C. The Lack of Federal Legislation Protecting Personal Data Generally

Comprehensive federal data protection regulation does not exist. Instead of passing a federal comprehensive privacy law that regulates the collection, processing, and use of data by all private companies, Congress has passed a multitude of sectoral legislation that regulates businesses operating within specific industries.[97] These laws include the Fair Credit Reporting Act (FCRA),[98] the Right to Financial Privacy Act (RFPA),[99] the Gramm-Leach-Bliley Act (GLBA),[100] the Children's Online Privacy Protection Act (COPPA),[101] and the Health Insurance Portability and Accountability Act (HIPAA).[102]

These sectoral laws are limited in applicability. For example, FCRA protections are limited to the disclosure of information that is collected for the purpose of establishing credit, employment, or insurance eligibility. [103] RFPA only protects against the disclosure of consumer financial records to other private companies or to the government.[104]

95. Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 506 (2010).

96. *See id.* at 505 (noting that courts have been reluctant to compensate plaintiffs for nonmonetary harms resulting from violations of privacy).

97. Paul M. Schwartz, *Privacy and Security Law: What Korean Companies Need to Know*, PAUL HASTINGS, http://www.paulhastings.com/area/privacy-and-cybersecurity/privacy-and-security-law-what-korean-companies-need-to-know (last visited Oct. 4, 2019).

98. Pub. L. No. 91-508, 84 Stat. 1114 (Oct. 26, 1970) (codified as amended at 15 USC §§ 1681-1681t (2018).

99. 12 U.S.C. §§ 3401–22 (2018).

100. Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (codified as amended in scattered sections of 12 and 15 U.S.C. (2018))

101. Pub. L. No. 105-277, 112 Stat. 2681 (Oct. 21, 1998) (codified as amended at 15 U.S.C. §§ 6501-06 (2018)).

102. Pub. L. No. 104-191, 110 Stat. 1936 (Aug. 21, 1996) (codified as amended in scattered sections of 26 and 42 U.S.C. (2018)).

103. James X. Dempsey and Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1477 (2004).

104. *Id.* at 1478. In 2003, RFPA was expanded to include all records of specified

Furthermore, the GLBA's privacy provision applies only to financial institutions,[105] while COPPA only applies to a website that *knowingly* collects, uses, or discloses personal information on children under thirteen.[106] Finally, although HIPAA provides strong protections,[107] it only applies to personally identifiable health information held by a covered entity.[108] Covered entities are narrowly defined, including only health plans, health care clearinghouses, and health care providers who electronically transmit health information in connection with a transaction.[109]

In addition to the aforementioned sectoral laws, the Federal Trade Commission (FTC) has broadly interpreted its power to regulate "unfair"[110] and "deceptive"[111] trade practices under Section 5 of the FTC Act to patrol data privacy violations.[112] Despite having the broadest

businesses, such as real estate agents, jewelers, car dealers, pawnshops, and travel agencies. *Id.*; *see also* CHARLES DOYLE, CONG. RESEARCH SERV., RL33320, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND 19 (2015), https://fas.org/sgp/crs/intel/RL33320.pdf (providing background information on the Right to Financial Privacy Act).

105. FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT 2 (2002), https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

106. Pub. L. No. 105-277, 112 Stat. 2681 (Oct. 21, 1998) (codified as amended at 15 U.S.C. §§ 6501-06 (2018)); *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions (last visited Dec. 10, 2019).

107. Pub. L. No. 104-191, 110 Stat. 1936 (Aug. 21, 1996) (codified as amended in scattered sections of 26 and 42 U.S.C.); *Health Insurance Portability and Accountability* Act, CAL. DEPT. OF HEALTH CARE SERVS., https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx (last visited Dec. 10, 2019).

108. *HIPAA Privacy Rule: Information for Researchers*, U.S. DEPT. OF HEALTH AND HUMAN SERVS.: NAT'L INSTS. OF HEALTH, https://privacyruleandresearch.nih.gov/pr_06.asp (last visited Oct. 10, 2019).

109. *Id.*

110. Unfair methods are defined as acts or practices that (1) cause or are likely to cause substantial injury to consumers that (2) are not reasonably avoidable by consumers, and (3) the injury is not outweighed by countervailing benefits to consumers. 15 U.S.C. § 45(n) (2018).

111. Deceptive acts or practices are defined as (1) material statements or omissions that (2) are likely to mislead consumers (3) acting reasonably under the circumstances. Letter from James C. Miller III, Chairman, Fed. Trade Comm., to Rep. John D. Dingell, Chairman, Comm. On Energy and Commerce 1–2 (October 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

112. Section 5 of the FTC Act states that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a) (2018).

power to regulate privacy violations across sectors, the FTC currently lacks the resources and authority necessary to adequately protect consumer privacy.[113]

As highlighted above, these laws do not cover most personal data that private companies collect, including shopping habits, religious affiliation, sexual preferences, locational data, sensitive health information, personal relationships, and other metadata.[114] Therefore, until the federal government passes a comprehensive privacy regulation, the responsibility for protecting most consumer data falls on the states, meaning that it is the Alaska legislature's responsibility to protect its citizens' data.

D. Potential Benefits to Companies Created By Comprehensive Privacy Law

A common argument against comprehensive privacy legislation is that the increased regulation will stifle innovation.[115] However, not all innovation should be encouraged, at least not without appropriate regulation and oversight. Innovation must be balanced against the potential harm it might cause. Innovation at the expense of safety and morality is generally deemed socially unacceptable. For example, twenty-two states and the District of Columbia have passed laws limiting the use of autonomous vehicles, citing concerns about safety.[116] These states have

113. The FTC does not have the ability to issue outright fines for unfair or deceptive trade practices. *See* 15 U.S.C. § 45(m)(1)(B) (explaining the FTC's remedial powers). Instead, it may only challenge these practices by initiating administrative adjudications. FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE, LAW ENFORCEMENT, AND RULEMAKING AUTHORITY (2019). The FTC's power to issue legislative, legally binding rules is extremely limited due to the overly burdensome rulemaking process that is required. Beth DeSimone & Amy Mudge, *Is Congress Putting the FTC on Steroids?*, SELLERBEWARE BLOG (Apr. 26, 2010), http://www.consumeradvertisinglawblog.com/2010/04/is-congress-putting-the-ftc-on-steroids.html; *see also* FED. TRADE COMM'N, OPERATING MANUAL § 7.2.3.1 (1971) ("Section 202(a) of Magnuson-Moss provides that the Commission's § 18 authority is its only authority to promulgate rules respecting unfair or deceptive acts or practices.").

114. CHERTOFF, *supra* note 2, at 73. Metadata is internet/telephonic addresses and routing instructions that identify the recipient and the sender of various materials over the internet or telephone. *Id.*

115. *See, e.g.*, DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 29 (2010), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf (noting that commenters on the Privacy and Innovation Notice of Inquiry expressed concerns that national legislation would stifle innovation).

116. Jack Karsten & Darrell West, *The State of Self-Driving Car Laws Across the*

determined that the risks posed by autonomous vehicles warrant increased regulation, despite the fact that this regulation will increase the cost to autonomous-vehicle-producing companies.[117] Another example is that most countries around the world have banned human reproductive cloning.[118] These countries have determined that the potential moral and ethical consequences that might result from human reproductive cloning outweigh the benefits of such an innovation, at least until the proper ethical framework can be developed to enable it.[119] Thus, certain limitations to innovation should be considered if the innovation raises safety or moral concerns, like those associated with unregulated data collection.[120]

Furthermore, increased regulation does not necessarily stifle innovation.[121] In fact, increased regulation can encourage positive innovation by incentivizing companies to actively seek solutions to problems that were previously ignored.[122] This is because, through regulation, companies are forced to work within specific limitations that did not previously exist.[123] For example, stringent emission standards accelerated the pace at which the automobile industry studied combustion, facilitating innovation in emission control and fuel economy.[124] Another more relevant example is privacy-enhancing technologies (PETs). PETs are generally "a class of technical measures [aimed] at preserving the privacy of individuals or groups of individuals."[125] PETs and other innovative solutions have already begun to emerge and to gain momentum due to laws such as the GDPR and the

U.S., BROOKINGS:TECHTANK (May 1, 2018), https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/.

117. *See id.* (noting safety concerns associated with autonomous vehicles).

118. *Cloning: Frequently Asked Questions*, NPR, https://www.npr.org/news/specials/cloning/faq_blanknav.html (last visited Dec. 18, 2019).

119. *See id.* (noting ethical concerns associated with human reproductive cloning).

120. *See supra* Section III.A.

121. *See* Roland Bastin & Georges Wantz, *The General Data Protection Regulation: Cross-Industry Innovation*, 15 INSIDE MAGAZINE 51, 52–53 (2017), https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-inside-magazine-issue-15-june-2017.pdf (discussing the promotion of innovation through the GDPR); *see also* Rob Atkinson & Les Garner, *Regulation as Industrial Policy: A Case Study of the U.S. Auto Industry*, 1 ECON. DEV. Q. 358, 363–371 (concluding that regulation incentivized innovation within the automobile industry).

122. *See* Bastin & Wantz, *supra* note 121, at 53 (noting that companies will continue to innovate with new rules in mind).

123. *Id.*

124. *See* Atkinson & Garner, *supra* note 121, at 364 (quoting a former Director of Vehicle Emissions at Chrysler).

125. Johannes Heurix et al., *A Taxonomy for Privacy Enhancing Technologies*, 53 COMPUTERS & SECURITY 1, 1 (2015).

CCPA.[126] For example, homomorphic encryption[127] schemes are becoming more prevalent because they allow companies to analyze data without compromising consumer privacy.[128]

Companies would also benefit from comprehensive privacy legislation because such a law would increase user trust. Many consumers recognize that companies are collecting vast amounts of data on them and are deeply anxious about how their personal information is used and protected.[129] In fact, current public opinion polls suggest that most Americans believe that their data is inadequately protected.[130] The polls also suggest that this lack of trust is causing consumers to provide incomplete or inaccurate data to data collectors.[131]

126. *See* THE ROYAL SOC'Y, PROTECTING PRIVACY IN PRACTICE: THE CURRENT USE, DEVELOPMENT AND LIMITS OF PRIVACY ENHANCING TECHNOLOGIES IN DATA ANALYSIS 4 (2019), https://royalsociety.org/-/media/policy/ projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf (noting the rise of PET).

127. Homomorphic encryption schemes enable a company to "run computations on encrypted data without decrypting it." Susan Miller, *Privacy Enhancing Technology for Data Analysis*, GCN (June 17, 2019), https://gcn.com/articles/2019/06/17/privacy-enhancing-technology.aspx.

128. *Id.*

129. *See* Timothy Morey et al., *Customer Data Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust ("It's not as if consumers don't realize that data about them is being captured, however; 97% of the people surveyed expressed concern that businesses and the government might misuse their data.").

130. *See, e.g.*, AKAMAI, CONSUMER ATTITUDES TOWARD DATA PRIVACY SURVEY 2018, (2018), https://www.akamai.com/us/en/multimedia/documents/report/akamai-research-consumer-attitudes-toward-data-privacy.pdf. The Akamai survey found that forty-two percent of respondents believed that web site operators did not care about using personal data responsibly or securely. *Id.* Another thirty-two percent answered "I think they mostly want to use our data in a responsible and secure way, but they're bad at it." *Id.* Only fourteen percent of respondents answered, "I think they're mostly good at using our data in responsible and secure way[s]." *Id.* Another survey found that "[t]wo percent of Americans expressed trust in social networking websites or applications; six percent trusted online retailers; and twelve percent to nineteen percent trusted federal or state governments, e-mail providers, and cellphone carriers. At the high end, twenty-six percent trusted health insurance companies, and thirty-nine percent trusted banks and credit card companies." NAT'L SCI. BD., SCIENCE & ENGINEERING INDICATORS 2018, 7–71, https://www.nsf.gov/statistics/2018/nsb20181/assets/404/science-and-technology-public-attitudes-and-understanding.pdf. Yet another study, conducted by the Pew Research Center, found that "[a] majority of Americans (64%) have personally experienced a major data breach, and relatively large shares of the public lack trust in key institutions—especially the federal government and social media sites—to protect their personal information." AARON SMITH, PEW RESEARCH CTR., AMERICANS AND CYBERSECURITY, (Jan.26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/.

131. *See, e.g.*, *Patients Holding Back Health Information Over Data Privacy Fears*, HIPAA J. (Jan. 5, 2017), https://www.hipaajournal.com/patients-holding-back-health-information-over-fears-of-data-privacy-8634/. A consumer poll,

The lack of consumer trust and data quality is concerning for private companies because trust is the cornerstone to many customer experiences.[132] Consumer trust has long been linked to customer satisfaction—which ensures greater customer retention—positive reviews and references, and improved financial outcomes for the company.[133] Additionally, consumer trust is more important than ever because consumers are bombarded with options—what was once a choice between a couple of brands is now a global mix of hundreds.[134] Compliance with privacy rules could become an effective marketing tool to distinguish one company from another.[135]

Furthermore, user trust promotes data quality.[136] Good-quality data is important for a myriad of reasons. First, it promotes reliable outputs by more accurately predicting consumer behavior.[137] These outputs enable companies to better predict consumer trends and develop products that maximize profit. Higher quality data also increases efficiency by decreasing the amount of time spent validating and correcting inaccurate data.[138] Finally, good-quality data allows companies to better market their products through more accurate targeting and communication.[139]

Due to the importance of data quality and consumer trust, companies should prioritize measures that will increase both. States can

completed by Black Book in 2016, found that eighty-seven percent of healthcare patients were unwilling to comprehensively share all of their health information with their providers. *Id.* Eighty-nine percent of consumers who had visited a healthcare provider in 2016 admitted to withholding some information during their visits. *Id.*

132. Blake Morgan, *How to Build Trust With Your Customers*, FORBES (June 11, 2018), https://www.forbes.com/sites/blakemorgan/2018/06/11/how-to-build-trust-with-your-customers/#2f76ca411cd3.

133. Chatura Ranaweea & Jaideep Prabhu, *On the Relative Importance of Customer Satisfaction and Trust as Determinants of Customer Retention and Positive Word of Mouth*, 12 J. OF TARGETING, MEASUREMENT & ANALYSIS FOR MKTG. 82, 89 (2003), https://link.springer.com/content/pdf/10.1057/palgrave.jt.5740100.pdf.

134. Vanessa Mitchell, *Why Customer Trust is More Vital to Brand Survival Than It's Ever Been*, CMO FROM IDG (June 12, 2018), https://www.cmo.com.au/article/642102/why-customer-trust-more-vital-brand-survival-than-it-ever-been/.

135. Companies are already beginning to emphasize privacy as a way to market their products to consumers. *See, e.g.*, Mike Wuerthele, *'Privacy. That's iPhone' Ad Campaign Launches, Highlights Apple's Stance On User Protection*, APPLEINSIDER (Mar. 14, 2019), https://appleinsider.com/articles/19/03/14/privacy-thats-iphone-ad-campaign-launches-highlights-apples-stance-on-user-protection.

136. Morey et al., *supra* note 129.

137. Hugo Moreno, *The Importance of Data Quality – Good, Bad or Ugly*, FORBES (June 5, 2017), https://www.forbes.com/sites/forbesinsights/2017/06/05/the-importance-of-data-quality-good-bad-or-ugly/#299fc96010c4.

138. *Id.*

139. *Id.*

increase user trust and data quality by adopting comprehensive privacy legislation. Polling suggests that adopting a policy that provides individuals with greater control over and protection of their data can increase public trust.[140] If Alaskans believe that the data they share online will be safe, they will be more likely to provide accurate data about themselves.[141] Therefore, private companies should welcome comprehensive data privacy legislation because its adoption could benefit private companies.

IV. AMERICAN VALUES CHANGE THE CALCULUS: CERTAIN ELEMENTS OF OTHER COMPREHENSIVE PRIVACY LAWS ARE LIKELY INCOMPATIBLE WITH AMERICAN VALUES

This Section will detail how the American conception of privacy is unique and how it substantially affects any proposed privacy legislation. The American conception of privacy focuses on privacy as liberty. The importance of liberty is perhaps even more overt in Alaska with the state's naturally rugged terrain and fiercely independent residents.[142] To better understand the American, and thus Alaskan, conception of privacy this Section will contrast the American conception with the European conception of privacy as dignity. Then it will argue that the American conception of privacy coupled with the prevalence of the First Amendment would likely prevent the adoption of a provision granting the right to be forgotten.

A. The Alaskan and American Conception of Privacy

The American conception of privacy is unique. For Americans, privacy focuses on protecting liberty.[143] The focus on liberty is perhaps even more distinct in Alaska, "the home of people who prize their individuality and who have chosen to settle or to continue living here in order to achieve a measure of control over their own lifestyles which is

140. *See, e.g.*, Abigail Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RESEARCH CTR.: FACTTANK (June 4, 2018), http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/. The Pew Research Center Survey conducted in 2015 found that ninety-three percent of Americans found it important to be in control of who can get information about them. *Id.* It also found that ninety percent of Americans also believed that controlling what information is collected about them is important. *Id.*

141. *Id.*

142. *See* Ravin v. State, 537 P.2d 494, 504 (Alaska 1975).

143. James Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004).

now virtually unattainable in many [other] states."[144] Privacy as liberty is best understood as the right to be free from unwanted government intrusions into private spaces, especially into one's home.[145] Liberty has evolved beyond spatial bounds to also protect freedom of belief, thought, and expression.[146] Yet American privacy law, however construed, still "tends to imagine the home as the primary defense, and the state as the primary enemy."[147] Generally, where American law recognizes a privacy violation, it is precisely because the government has involved itself in the matter.[148] Thus, the less involved the government is in an alleged privacy violation and the further it is from one's home, the less likely the violation will be recognized.[149]

To better understand the American and Alaskan conception of privacy, it is helpful to contrast it with the European Union's conception of privacy. Whereas the American notion of privacy focuses on privacy as liberty, the European conception centers on privacy as dignity.[150] The Europeans' conception of privacy as dignity is best understood as the "right to one's image, name, and reputation."[151] What matters to Europeans is the right to control their public image. European privacy law, specifically the right to be forgotten, has developed to protect a kind of personhood where every person, no matter his or her social status, has the right to a respectable public image.[152]

Additionally, the United States Constitution does not provide an explicit right to privacy.[153] Federal privacy rights have thus been implied by the Supreme Court's interpretation of the Constitution.[154] This

144. *Ravin*, 537 P.2d at 504.

145. Susan P. Stuart, *Fun with Dick and Jane and Lawrence: A Primer on Education Privacy as Constitutional Liberty*, 88 MARQ. L. REV. 563, 572 (2004).

146. *Id.* The freedoms of thought, belief, and expression are encompassed in the First Amendment. Section IV.B *infra* describes how the First Amendment has influenced the development of American privacy law.

147. Whitman, *supra* note 143, at 1215.

148. *Id.*

149. *See id.* at 1194–95 (explaining how privacy protections are significantly more limited outside the home).

150. *Id.* at 1161.

151. *Id.* at 1167.

152. *Id.* at 1211 ("[Dignity is defined as a] certain kind of personhood: a kind of personhood founded in the commitment to a society in which every person, of every social station, has the right to put on a respectable public face.").

153. *Compare* U.S. CONST. *with* Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326), ch. II, art. 8; *see also* Ryan Moshell, *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH. L. REV. 357, 373 (2005) (describing the lack of an explicit right to privacy in the United States).

154. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (finding the right to privacy through the penumbras of enumerated rights in the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments); Roe v. Wade, 410 U.S. 113 (1973);

approach is inherently limiting because rights explicitly recognized by the United States Constitution will always supersede privacy rights. Although the Alaska Constitution recognizes an explicit right to privacy, these rights must not conflict with rights expressly recognized by the Federal Constitution.[155] Therefore, even if the Alaska legislature passed legislation that was consistent with the Alaska Constitution, the law could be struck down federally if it is considered inconsistent with the Federal Constitution.

B. The Right to Be Forgotten

Any proposed law should exclude the right to be forgotten. The right to be forgotten, a uniquely European concept arising from the European conception of privacy as dignity,[156] enables a consumer to request that a business delete all data pertaining to him that is no longer necessary for a legitimate business or legal purpose.[157]

The adoption of a right to be forgotten would likely be incompatible with the First Amendment. The First Amendment generally prevents the government from passing laws that control or limit the dissemination of information.[158] Occasionally, an individual's privacy expectations conflict with the dissemination of information. In conflicts between privacy expectations and the First Amendment, the First Amendment almost always prevails.[159] The First Amendment's dominance arises from its

Lawrence v. Texas, 539 U.S. 558 (2003).

155. *See* U.S. CONST. art. IV (establishing that the federal constitution, and federal law generally, take precedence over state laws and constitutions).

156. *See generally* Whitman, *supra* note 143 (discussing the differences between the American conception of privacy and the European conception).

157. *GDPR: Right to be Forgotten*, INTERSOFT CONSULTING, https://gdpr-info.eu/issues/right-to-be-forgotten/ (last visited Dec. 16, 2019). This concept is a key component of the GDPR. However, the concept existed long before it was explicitly written into law. For example, in *Google v. Spain*, the European Court of Justice ruled that European citizens have the right to request that companies operating commercial search engines that gather personal information for profit, such as Google, remove links to personal information. Opinion of Advocate General Jääskinen, Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2013 E.C.R. 424.

158. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1050–51 (2000).

159. *See, e.g.*, Time, Inc. v. Hill, 385 U.S. 374, 389 (1975) (holding that unless there is a finding of malicious intent, press statements are protected under the First Amendment even if they are otherwise false or inaccurate); N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964) (holding that news publications could not be liable for libel of public officials unless there is proof of actual intent or recklessness); Sipple v. Chronicle Publishing Co., 154 Cal. App. 3d 1040, 1048–49

modern interpretation dictating that newsworthy information—information of legitimate public interest—should be uninhibited.[160] Thus, once data about any individual has been made public, it is extremely difficult to remove it.

Further complicating the constitutionality of the right to be forgotten is the commercial speech doctrine[161] and the Supreme Court's ruling in *Citizens United v. Federal Election Commission*.[162] Traditionally, the Court has applied a more relaxed version of its First Amendment tests to commercial speech, relying on a form of intermediate scrutiny.[163] More recently, in *Citizens United*, the Supreme Court determined that corporations are entitled to the same First Amendment protections as natural persons or traditional press companies.[164] Under this decision, the First Amendment has expanded beyond protecting only the individual and the media.[165] Now the First Amendment protects corporations not only when they use information to express themselves and to keep the public informed, but also when they use data to market products.[166]

Even though Alaska, much like the European Union, recognizes an explicit right to privacy, this does not permit Alaska to promote this right

(1984) (holding that a newspaper's right to publish intimate information outweighed Sipple's right to keep his sexual orientation a secret because the information became newsworthy after Sipple became a national hero for preventing President Ford's assassination).

160. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1155 (2005) (quoting N.Y. Times Co. v. Sullivan, 376 U.S. at 270); *see generally*, Erin C. Carroll, *Making News: Balancing Newsworthiness and Privacy in the Age of Algorithms*, 106 GEO. L.J. 69 (2017) (discussing how the press has used the broad definition of newsworthiness to shield itself against invasion of privacy lawsuits).

161. The commercial speech doctrine is a tricky doctrine without a concrete definition. Kathryn E. Gilbert, *Commercial Speech in Crisis: Crisis Pregnancy Center Regulations and Definitions of Commercial Speech*, 111 MICH. L. REV. 591, 596 (2013). However, if the speech "proposes a commercial transaction," or is "related solely to the economic interests of the speaker," it is considered commercial speech. *Id.* at 598.

162. 558 U.S. 310 (2010).

163. If the court determines that the speech in question is commercial speech, then the regulation curtailing such speech would have to directly advance the asserted government interest, and the regulation must be narrowly tailored. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 564–65 (1980).

164. 558 U.S. at 365–66.

165. *See id.* at 319 ("The Government may regulate corporate political speech through disclaimer and disclosure requirements, but it may not suppress that speech altogether.").

166. *Id.*; *see also* Eugene Volokh, *Freedom for the Press as an Industry, or For the Press as a Technology? From the* Framing *to Today*, 160 U. PA. L. REV. 459, 538–39 (2012) (noting that the Supreme Court continues to provide equal treatment to speakers without regard to whether they are members of the press); United States v. Caronia, 703 F.3d 149, 168–69 (2nd Cir. 2012) (holding that off-label promotion of FDA-approved drugs is protected by the First Amendment).

at the expense of the First Amendment. The First Amendment provides broad protection of expression. Thus, the right to be forgotten is not easily defensible under the First Amendment's current interpretation. However, legislation in Alaska could include a number of other privacy protections that would sufficiently address the underlying concerns driving the right to be forgotten. These possibilities are discussed in the following Section.

V. WHAT THIS PRIVACY LEGISLATION SHOULD INCLUDE

This Section will discuss what the Alaska legislature should include in its comprehensive privacy law. It will begin by arguing that any comprehensive privacy law should be grounded in the Asian-Pacific Economic Cooperation (APEC) privacy principles.[167] It will then describe specific elements that should be included, using the CCPA[168] and the GDPR[169] for guidance.

A. Establishing a Strong Foundation: Utilization of a Commonly Accepted Framework

The privacy legislation should be grounded in a set of broadly applicable principles predicated on the APEC privacy principles.[170] The APEC privacy principles include broad notions such as notice, the prevention of harm, collection limitation, use limitation, choice, maintenance of the integrity of personal information, security safeguards, and accountability.[171] Grounding legislation in the APEC privacy principles will provide a strong base of data protection and user control,

167. ASIA-PACIFIC ECON. COOPERATION, APEC PRIVACY FRAMEWORK 2015 (2017).

168. CAL. CIV. CODE §§ 1798.100–199 (2019).

169. Council Regulation 2016/679, art. 4, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

170. Though the Fair Information Privacy Principles (FIPPs) and the Organisation for Economic Co-operation and Development (OECD) privacy principles are more commonly used when discussing privacy principles, I chose the APEC privacy principles because I found their language more appealing. The APEC privacy principles are essentially the same as the OECD privacy principles; however, I prefer their phrasing over the OECD privacy principles. *See* Andrei Gribakov, *Cross-Border Privacy Rules in Asia: An Overview*, LAWFARE (Jan. 3, 2019), https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview (noting the similarities between the APEC privacy principles and the OECD principles).

171. *See* ASIA-PACIFIC ECON. COOPERATION, *supra* note 167, at 10–22 (listing the APEC principles).

while simultaneously providing the legislature with a sound starting point that other nations around the world have used. Thus, the Alaska legislature should consider utilizing the APEC privacy principles as the foundation of any proposed legislation.

First, the Alaska law should require companies to develop data collection and use policies and procedures that prevent data's misuse.[172] Specifically, the companies should be required to consider the risks associated with the use of personal data and take proportionate measures to mitigate the harm based on the likelihood and severity of harm threatened by such use.[173] The required compliance program should compel companies to provide clear and easily accessible statements about their data privacy policies before or at the time that personal data is collected.[174] If the statement cannot be provided before or at the time of collection, then the company should provide it as soon as practicably possible after collection.[175] Upon completion of a risk analysis, companies should limit collection to information that is relevant to a specific purpose that is both lawful and fair.[176]

Once the data is collected, companies should limit the use of the collected data to circumstances that fulfill the original purposes of collection (unless the individual provides consent), to provide a service or product requested by the consumer, or to meet a legal obligation.[177] Companies should also ensure that consumer information is accurate, complete, and up-to-date.[178] Additionally, companies should implement appropriate safeguards to minimize loss or unauthorized access, use, modification, or disclosure of personal information.[179] These safeguards should balance the likelihood and severity of harm resulting from usage of the personal data, the context in which the data is stored, and the data's sensitivity.[180] The safeguards should be periodically reassessed and

172. *See id.* at 10 (recognizing the need to prevent the misuse of such sensitive information).
173. *Id.* at 10–11.
174. *See id.* at 11 (noting that statements should include "a) the fact that personal information is being collected; b) the purpose for which personal information is collected; c) the types of persons or organizations to whom personal information might be disclosed; d) the identity and location of the personal information controller . . . ; e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.").
175. *Id.* at 12.
176. *Id.* at 13. Notice to and consent of the individual should be provided during collection, where appropriate. *Id.* at 14.
177. *Id.* at 14.
178. *Id.* at 17.
179. *Id.*
180. *Id.*

reviewed.[181]

Second, the law should provide consumers with certain explicit rights. The law should empower consumers to exercise some choice regarding the collection, use, and disclosure of their information through clear, prominent, accessible, and affordable mechanisms.[182] Consumers should also be able to obtain confirmation from the controller of whether it holds personal information about them.[183] Upon provision of sufficient proof of identity, the company should provide the individual with the requested data.[184] The company should also provide consumers with the right to correct, complete, or amend information about them.[185] This ensures that the data retained by companies on individuals is accurate and up to date. If the company denies a request, it should provide reasons for its denial and an opportunity for the consumer to appeal the decision.[186]

Finally, the law should ensure that companies are held accountable for compliance with the aforementioned principles. Thus, the law must contain enforcement provisions that facilitate compliance. Companies should also be required to exercise due diligence and take reasonable steps, when transferring data, to ensure that the recipient sufficiently protects personal information.[187]

Compliance with the APEC privacy principles will provide a solid foundation upon which to build. These principles not only ensure an adequate level of data protection, but also provide for some commonality among jurisdictions that have already passed privacy regulation.[188] Thus,

181. *Id.*
182. *Id.* at 15.
183. *Id.* at 17–18.
184. *Id.* at 18. The requested data should be provided at a non-excessive charge, in a reasonable manner, and in a generally understandable form. *Id.*
185. *Id.* These right should be provided so long as compliance with such request is not unreasonable or disproportionate to the individual's privacy risk. *Id.*
186. *Id.* at 19.
187. *Id.* at 22.
188. *See, e.g.*, GDPR, *supra* note 169; Lei Geral de Proteção de Dados Lei No. 13, 709, de Agosto 14, 2018, Aug. 15, 2018 (Braz.) [hereinafter LGPD]; Kojin Joho No Hogo Ni Kansuru Horitsu [Act on the Protection of Personal Information], Law No. 57 of 2003 (Japan), translated in Amended Act on the Protection of Personal Information (Tentative Translation), Pers. Info. Protection Commission (Dec. 2016) [hereinafter APPI], https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf. Though the GDPR, the LGPD, and the APPI have their differences, at their core they are founded on the same principles as the GDPR—the OECD privacy principles. *See* Kensaku Takase, *GDPR Matchup: Japan's Act on the Protection of Personal Information,* IAPP (Aug. 29, 2017), https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/ (noting the similarities between the GDPR and the APPI); *What is the LGPD? Brazil's Version of the GDPR*, GDPR.EU, https://gdpr.eu/gdpr-

Alaska's legislature should consider grounding any privacy legislation in these principles.

B. Incentivizing Compliance Through Strong Penalties

The Alaska legislature should include significant penalties for noncompliance in its privacy legislation. In this context, significant means reasonably calculated to effectively influence a business's decision-making calculus, without being excessive. A significant penalty will ensure that the businesses are not simply deciding that the fine for violating the legislation is more favorable than not collecting, using, or selling a consumer's data. The actual or threatened imposition of sanctions can deter corporate wrongdoing. Because corporate activity is generally undertaken to achieve some economic benefit, corporate executives normally make business decisions based on calculations of potential economic costs and benefits.[189] Therefore, high economic penalties for non-compliance could be effective in deterring companies from violating the law.

Both California and the European Union have crafted legislation with significant penalty provisions. The Alaska legislature should look to these models when crafting its own penalty structure. The GDPR has the most extensive penalty structure, providing both a private right of action and hefty administrative fines for *any* violation of rights explicitly provided by the GDPR.[190] Therefore, a company might be liable for paying both administrative fines and civil damages for the same violation. The CCPA, on the other hand, has far weaker penalties for violations. Under the CCPA, no administrative agency has the power to impose administrative fines.[191] Furthermore, it only provides a private right of action under a narrow scope of circumstances: for example, when a company fails to implement and maintain reasonable security procedures.[192]

The Alaska legislature should consider adopting a position that lies somewhere between these two approaches. Instead of adopting a private right of action for *all* violations of the law, the Alaska legislature should

vs-lgpd/ (last visited May 29, 2020) (noting the similarities between the GDPR and LGPD). The APEC privacy principles are derivative of the OECD privacy principles. Gribakov, *supra* note 170. Thus, grounding Alaska's privacy law in the APEC privacy principles will reduce compliance costs by ensuring core similarities with other international privacy regimes.

189. Charles R. Nesson, *Developments in the Law: Corporate Crime: Regulating Corporate Behavior Through Criminal Sanctions*, 92 HARV. L. REV. 1227, 1235 (1979).

190. GDPR *supra* note 169, at art. 79, 83.

191. *See generally* CAL. CIV. CODE §§ 1798.100–1798.199 (2019).

192. *Id.* § 1798.150.

include a private right of action for violations of reasonable security practices, similar to what exists under the CCPA. Unlike the CCPA, the Alaska law should grant an administrative agency the authority to issue fines for any violation of Alaska's privacy legislation. This approach should incentivize compliance without being overly burdensome by forcing companies to pay administrative fines *and* litigation expenses for the same violation. Citizens will be incentivized to hold companies accountable for data breaches resulting from poor data protection policies, while an administrative body will be responsible for enforcing all other violations of the act. An additional benefit of the bifurcation of responsibility is that it will reduce the future administrative agency's budgetary needs. Instead of having to enforce all areas of the law, it will only need to focus on enforcing violations not covered under data breach litigation.

C. Financial Incentives

Another provision that the legislature should consider borrowing from existing privacy legislation is the CCPA's financial incentives provision. The CCPA provides that "[a] business may offer financial incentives . . . for the collection of personal information, the sale of personal information, or the deletion of personal information."[193] Financial incentives have proven successful in increasing and maintaining participation in other areas and could prove useful in encouraging consumers to part with their data.

For example, financial incentives have been shown to increase participation in physical activity promotion programs utilizing activity trackers.[194] Financial incentives, such as profit sharing, project and scheduled bonuses, and stock options and warrants have also been effective in motivating higher levels of performance and productivity in employees.[195] Therefore, the adoption of a provision permitting private entities to offer financial incentives for the collection, sale, or disclosure

193. *Id.* § 1798.125(b)(1).

194. *See* Jan-Niklas Kramer et al., *A Cluster-Randomized Trial on Small Incentives to Promote Physical Activity*, 56 AM. J. PREVENTATIVE MED. e45, e48 (2019) (noting that the personal financial incentive group had 5.94% participation, while the control group had 3.23% participation).

195. Adam Grant & Jitendra Singh, *The Problem with Financial Incentives – and What to Do About It*, U. PA. (Mar. 30, 2011), https://knowledge.wharton.upenn.edu/article/the-problem-with-financial-incentives-and-what-to-do-about-it/; *see also* ANDREW BALLENTINE ET AL., THE ROLE OF MONETARY AND NONMONETARY INCENTIVES IN THE WORKPLACE AS INFLUENCED BY CAREER STAGE 1–2 (2019), https://edis.ifas.ufl.edu/pdffiles/HR/HR01600.pdf (discussing the value of monetary and nonmonetary incentives).

of personal information could have similarly positive results of increasing voluntary participation.

D. Miscellaneous Practical Considerations

Other important aspects that should be incorporated into the legislation include practical provisions that will maximize its positive impact. The legislation should include a public policy exemption provision, a provision that encourages the designated supervisory authority to work with companies to achieve compliance, and a provision that limits the scope of the law.

The legislation should include a public policy exception that enables companies to more freely collect, use, store, and disclose information if it is necessary for research purposes, public health reasons, or for the completion of a government contract.[196] Scientific research and public welfare are of vital importance to society and should be appropriately balanced with privacy concerns. Furthermore, the government has become increasingly dependent on private contractors; thus, the bill should not prevent the government from functioning properly.[197] Therefore, a public policy exemption would ensure that the legislation does not unduly obstruct government operations, hinder scientific and historical research, or harm public health.

Additionally, the legislation should include a provision that encourages the designated supervisory authority to work with companies to understand and become compliant with its provisions. It should be clear that the supervisory authority's mission is not to mercilessly punish violators. Instead, the regulatory authority should understand its duty to help, guide, and inform companies about the legislation and upcoming regulatory developments, utilizing reasonable fines only as a last resort. Including this provision will make the supervisory authority's objective clear. It would also calm businesses' fear that the supervisory authority will seek only to punish violators without providing sufficient guidance.

Finally, the legislation should be limited to larger companies. The Alaska legislature should consider adopting a provision similar to that included within the CCPA that limits the scope of the CCPA. Similar to the CCPA, the Alaska law should be limited to companies that do

196. *See, e.g.*, GDPR, *supra* note 169; CAL. CIV. CODE §§ 1798.100–1798.199 (2019).

197. *See* Steven L. Schooner & Danieal S. Greenspahn, *Too Dependent on Contractors? Minimum Standards for Responsible Governance*, J. CONT. MGMT. 9, 10–12 (2008) (explaining the federal government's increased reliance on contract workers).

business in Alaska and collect consumer personal information.[198] It should also consider adopting a requirement similar to the CCPA that requires a company to satisfy one of the following before being covered by the law: the company (1) has over $25 million in annual gross revenue; (2) collects, processes, or sells the consumer information of 50,000 or more Alaska residents; *or* (3) derives fifty percent or more of its annual revenue from selling personal data.[199] Limiting the scope of the law in such a way will enable small companies to form and grow without being prematurely crushed by overly burdensome regulations.

VI. CONCLUSION

Because the Alaska Constitution explicitly protects the privacy rights of its citizens and instructs the legislature to implement these rights, Alaska's legislature should adopt comprehensive privacy legislation. This legislation would protect Alaska citizens from privacy violations perpetrated by private actors. Comprehensive privacy legislation is necessary because current state law provides insufficient protection and federal comprehensive privacy legislation does not exist. In order for the legislation to be effective, it should be based in the APEC principles, create a strong enforcement regime, offer financial incentives, consider public policy implications, and encourage a regulatory environment that is focused on working with the private sector to increase compliance rather than simply punish violators. Finally, the legislature should consider cultural norms and values while crafting the legislation. If comprehensive privacy legislation is correctly drafted, it would promote Alaska's constitutional right to privacy by protecting its citizens from perhaps the most frequent perpetrators of privacy violations—private entities.

198. *See* CAL. CIV. CODE § 1798.140.
199. *See id.*